**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

Some types of physical security measures that can be put into place include alarms and locks.

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

* At least eight digits long
* Include non-alphabetic characters
* Make sure it’s not easy to guess
* Change it every month

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters incoming information through an internet connection into an organisation’s internal network.

1. What are the main purposes of firewalls and how are these purposes achieved?

The main purpose of firewalls is to block any potential security risks to the network. It can also be used to restrict unauthorised access to confidential information. These are achieved by using two separate NICs.

1. Why do firewalls use 2 separate NICs?

Firewalls use two separate NICs; one connects to the internal network and the other connects to the outside world. Material can only be moved by from one to the other by CPU of the server that is acting as the firewall. The firewall checks the data and information for authenticity, viruses and other malicious codes. Using two NICs keeps the network safer from outside threats.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware is malicious software; it includes spyware, adware, Trojan horses, worms and viruses. Antivirus software, anti-adware programs and firewalls are used to protect against malware.

**Encryption**

1. What is encryption?

Encryption is the process or translating data into secret code that can only be read by authorised users.

1. Describe the nature of WPA or WPA2.

WPA and WPA2 also known as wi-fi protected access is a security protocol for use by wireless LANs. It provides security by encrypting data sent over radio waves so that it is protected during transmission between devices.

1. What is encrypted data known as?

Encryption is known as ciphertext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

The protocol to allow secure financial transactions across the internet is knows as hypertext transfer protocol security or HTTP. It is a secure protocol between client’s web browser and the web server to ensure that the connection is established and maintained. Transmissions are encrypted and authenticated as they are transmitted.

1. What is digital identification certificate technology based on?

Digital identification certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

1. Describe the nature of Secure sockets layer (SSL) protocol.

Secure sockets layer protocol is a cryptographic protocol that provides secure connection on the internet.

**Physical design of networks**

1. What is the role of a network diagram?

The role of the network diagram is so that people working in tech support know where everything in the network is located.